IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

COURTNEY DIANA, individually and on behalf of all others similarly situated,	
Plaintiff,	
v.	**Case No:**
HORIZON HEALTHCARE SERVICES, INC., d/b/a HORIZON BLUE CROSS BLUE SHIELD OF NEW JERSEY, a New Jersey corporation,	**JURY TRIAL DEMANDED**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Courtney Diana ("Plaintiff"), on behalf of herself and all others similarly situated, by and through her attorneys, brings this action against Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey ("Horizon" or "Defendant"), and alleges as follows:

NATURE OF THE CASE

1. This is a national consumer class action lawsuit brought by Plaintiff, individually and on behalf of all other similarly situated persons (*i.e.*, the Class Members), who are consumers of health insurance coverage and whose personally identifiable information and personal health information (collectively referred to as "PII/PHI") entrusted to Horizon was stolen by a thief or thieves while in the possession, custody, and control of Horizon.

2. PII/PHI includes Plaintiff's and Class Members' names, addresses, dates of birth, Social Security numbers, member identification numbers, and clinical information.

3. On or about November 1, 2013, two laptop computers containing the PII/PHI of Plaintiff and more than 839,000 Class Members were taken from a Horizon office in Newark, New Jersey (the "Data Breach").

4. Horizon flagrantly disregarded Plaintiff's and Class Members' privacy rights by intentionally, willfully, recklessly, and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure. Plaintiff's and Class Members' PII/PHI was improperly handled and stored, was unsecured, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class Members' PII/PHI was compromised and stolen.

5. Horizon's intentional, willful, reckless, and/or negligent disregard of Plaintiff's and Class Members' rights directly and proximately caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties can have a serious adverse impact on, among other things, a victim's credit rating and finances. The type of wrongful PII/PHI disclosure made by Horizon is of the most harmful because it generally takes a significant amount of time for a victim to become aware of misuse of the disseminated PII/PHI.

6. On behalf of herself and Class Members, Plaintiff has standing to bring this lawsuit because her PII/PHI was included in the Data Breach and she was damaged as a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach.

7. Horizon's wrongful actions and inaction and the resulting Data Breach have, *inter alia*, placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[1] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who may now possess Plaintiff's and Class Members' PII/PHI have not yet used the information but will do so later, or re-sell it. Even without such loss, Plaintiff and Class Members are entitled to relief and recovery, including statutory damages under federal statutory provisions, as set forth herein.

8. Horizon's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA"). Horizon failed to

[1] According to the United States Government Accounting Office ("GAO"), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

adopt, implement, and maintain adequate procedures to protect such information and limit the dissemination of same to the permissible purposes under FCRA. In further violation of FCRA, Horizon failed to protect and wrongfully disseminated Plaintiff's and Class Members' PII/PHI, which is "medical information" specifically protected by FCRA. As a direct and proximate result of Horizon's willful, reckless, and/or grossly negligent violations of FCRA, an unauthorized third party (or parties) obtained Plaintiff's and Class Members' PII/PHI for no permissible purpose under FCRA.

9. Horizon's wrongful actions and inaction and the resulting Data Breach also constitute common law negligence, common law invasion of privacy by public disclosure of private facts, and unjust enrichment.

10. Plaintiff, on behalf of herself and Class Members, seeks actual damages, economic damages, statutory damages, nominal damages, exemplary damages, injunctive relief, attorneys' fees, litigation expenses, and costs of suit.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiff's FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction

over Horizon because at all relevant times, Horizon conducted (and continues to conduct) substantial business in the District of New Jersey.

12. Venue is proper in the District of New Jersey pursuant to 28 U.S.C. § 1391(b) and (c), because a substantial part, if not all, of the events giving rise to this action occurred in the District of New Jersey and Horizon resides, is located, can be found, and conducts substantial business in the District of New Jersey.

PARTIES

13. Plaintiff Courtney Diana ("Plaintiff") is a New Jersey citizen residing in the District of New Jersey. Plaintiff has health insurance with Horizon through her employer. Plaintiff pays for a portion of her Horizon health insurance premiums, which are deducted directly from her paycheck. On or about December 10, 2013, Plaintiff was advised that her PII/PHI was on the laptop computers stolen and compromised in the Data Breach.

14. Plaintiff's PII/PHI, which she entrusted to Horizon and which Horizon failed to properly safeguard and protect, was stolen from Horizon on or about November 1, 2013.

15. As a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, Plaintiff has suffered (and will continue to suffer) economic damages and other actual harm, including, but not limited to, emotional distress over learning of the theft of her PII/PHI, the general inconvenience and annoyance of dealing with her stolen, compromised and disseminated PII/PHI, and statutory damages under FCRA. Horizon's wrongful disclosure of, and failure to safeguard and protect, Plaintiff's PII/PHI has also placed her at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

16. Defendant Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey, is a health insurance company with approximately 3.7 million members, with its company headquarters in Newark, New Jersey.

17. Horizon "provides medical insurance products and services to individuals and employers in New Jersey. The company offers Medicare and Medicaid, prescription drug (Rx), and health and wellness insurance products and services. Horizon . . . , through its subsidiaries, also sells dental insurance products for individuals and groups in New York and Pennsylvania; and worker compensation and personal injury protection administrative services and access to life insurance products."[2]

18. At all relevant times, Horizon was (and continues to be) entrusted with, and obligated to safeguard and protect, Plaintiff's and Class Members' PII/PHI in connection with the insurance products purchased and/or sought to be purchased by Plaintiff and Class Members in consumer transactions during the Class Period—to wit, in order to purchase and/or seek to purchase insurance products sold by Horizon, Plaintiff and Class Members were required to provide (or have provided) their PII/PHI to Defendant.

19. Horizon handles Plaintiff's and Class Members' PII/PHI in numerous ways, including, *inter alia*: 1) maintaining the PII/PHI for its own files; and 2) submitting the PII/PHI to third parties for purposes of, *inter alia*, providing payment for health care services provided to Plaintiff and Class Members, setting rates for health insurance, and setting rates for the payment of certain health care services.

[2] http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=4001320 (last visited Dec. 10, 2013).

20. Horizon also assembles Plaintiff's and Class Members' PII/PHI and transmits it to third parties for purposes of determining whether Plaintiff and Class Members are eligible for various medical treatments and the insurance coverage of such treatments.

BACKGROUND FACTS

21. In the regular course of its business, Horizon collects and maintains possession, custody, and control of a wide variety of personal and confidential information, including Plaintiff's and Class Members' PII/PHI, for purposes of providing quotes and the sale of health insurance.

22. Horizon stored Plaintiff's and Class Members' PII/PHI, at a minimum, in an unencrypted format on two (2) laptop computers, which is against industry practices and in violation of the Health Insurance Portability and Accountability Act of 1996 ("HIPPA").

23. Horizon does not know the whereabouts of the laptop computers.

24. The laptop computers contain the unencrypted PII/PHI of Plaintiff and over 839,000 Class Members, all of whom are (or were) Horizon patients.

25. According to Horizon, it has 24-hour, 7 days a week security at its Newark offices where the Data Breach occurred, and "[n]o one can gain access to the building without a valid reason for being there. Whoever stole the two laptops was in the building for a legitimate purpose. The laptops were tethered by cable locks to the employees' workstations. The locks were disabled. Our security cameras did not capture the theft."[3]

[3] Marianne K. McGee, "Unencrypted Laptops Lead to Mega-Breach," Data Breach Today (Dec. 9, 2013), available at http://www.databreachtoday.com/unencrypted-laptops-lead-to-mega-breach-a-6277 (last visited Dec. 10, 2013).

26. The facts surrounding the Data Breach demonstrate that the stolen laptop computers were likely targeted due to the storage of Plaintiff's and Class Members' highly sensitive and private PII/PHI on them.

27. Despite knowing about the Data Breach since at least November 4, 2013, Horizon did not begin formally notifying Plaintiff and Class Members of the Data Breach until December 6, 2013—more than one month after the theft of the laptop computers.

28. During the intervening period between the Data Breach and the date the first wave of notification letters was sent to Plaintiff and Class Members, their unencrypted PII/PHI could have been bought and sold several times on the robust international cyber black market while they had no chance whatsoever to take measures to protect their privacy.

29. In the aftermath of the Data Breach, Horizon allegedly "has set up safeguards to prevent a similar incident in the future—including tougher policies and stronger encryption processes"[4] that could have been implemented prior to the Data Breach and prevented it.

30. Horizon's wrongful actions and inaction—to wit, failing to protect Plaintiff's and Class Members' PII/PHI with which it was entrusted—directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' unencrypted PII/PHI without their knowledge, authorization, and consent. As a further direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other actual harm including, without limitation: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses

[4] "Horizon Policyholders Warned Of Data Breach From Stolen Laptops," CBS New York (Dec. 7, 2013), available at http://newyork.cbslocal.com/2013/12/07/horizon-policyholders-warned-of-possible-identity-theft-from-stolen-laptops/ (last visited Dec. 10, 2013).

incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation.

31. Notwithstanding Horizon's wrongful actions and inaction and the resulting Data Breach, Horizon has offered a mere one year of credit monitoring and identity theft protection services, which is insufficient given the trove of unencrypted PII/PHI taken and disseminated to the world and the manipulation and machinations of cyber criminals.

32. As a direct and proximate result of Horizon's failure to properly safeguard and protect Plaintiff's and Class Members' PII/PHI, including, *inter alia*, failing to secure the stolen laptop computers, failing to encrypt their PII/PHI, and violating standard industry practices and protocols for protecting PII/PHI, Plaintiff's and Class Members' privacy has been (and will continue to be) invaded and their rights violated. Their compromised PII/PHI was private and sensitive in nature and was left inadequately protected and unencrypted by Horizon. Horizon's wrongful actions and inaction and the resulting Data Breach have placed Plaintiff and Class Members at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud.

33. Adding to the culpability and willfulness, recklessness, and/or negligence of Horizon's conduct and its violation of numerous industry standards and HIPPA, is the fact that Horizon previously suffered a data breach in 2008 when an unsecure Horizon laptop computer

containing nearly identical information for 300,000 of its insureds was stolen.[5] Horizon, however, failed to learn from its previous misconduct.

34. Identity theft occurs when a person's PII, such as the person's name, e-mail address, address, Social Security number, billing and shipping addresses, phone number and credit card information is used or attempted to be used without his or her permission to commit fraud or other crimes.[6]

35. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[7] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[8]

36. The FTC estimates that the identities of as many as 9 million Americans are stolen each year. *Id.*

37. As a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members will now be required to take the time and

---

[5] *See* http://ivebeenmugged.typepad.com/my_weblog/pdf/Horizon_notice_Feb2008.pdf (last visited Dec. 9, 2013); http://www.givemebackmycredit.com/blog/2008/02/laptop-stolen-containing-data.html (last visited Dec. 10, 2013).

[6] *See* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Dec. 10, 2013).

[7] *Protecting Consumer Privacy in an Era of Rapid Change* FTC Report (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Dec. 10, 2013).

[8] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35–38 (Dec. 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited Dec. 10, 2013); *Comment of Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12.

effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. Because Plaintiff's and Class Members' Social Security numbers were stolen and compromised, as well as their medical information, they also now face a significantly heightened risk of identity theft, identity fraud, and medical fraud.

38. According to the FTC, identity theft is serious. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[9]

39. Theft of medical information, such as that included in the Data Breach here, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[10]

40. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike

---

[9] *See* Federal Trade Commission, *Signs of Identity Theft*, http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited Dec. 10, 2013).

[10] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Dec. 10, 2013).

other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

41. Identity thieves also use Social Security numbers to obtain false identification cards, obtain government benefits in the victim's name, commit crimes, and file fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

42. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[11] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

43. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems.

[11] *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327, available at http://www.ssa.gov/pubs/10064.html (last visited Dec. 10, 2013).

Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

44. As a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, the thieves and/or their customers now have Plaintiff's and Class Members' PII/PHI. As such, Plaintiff and Class Members have been deprived of the value of their PII/PHI.[12]

45. Plaintiff's and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[13] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[14]

---

[12] *See, e.g.,* John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted);

ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited Dec. 10, 2013).

[13] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

[14] StopTheHacker, *The "Underground Credit Card Blackmarket*, available at http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Dec. 10, 2013).

46. It is reported that "medical records hold an average black market value of $50 per record."[15]

47. The Data Breach was a direct and proximate result of Horizon's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiff's and Class Members' PII/PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations and industry practices, as well as common law duties.

48. Horizon flagrantly disregarded and violated Plaintiff's and Class Members' privacy rights, and materially harmed them in the process, by not obtaining Plaintiff's and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by HIPAA and other pertinent laws, regulations, industry standards and internal company standards.

49. Horizon flagrantly disregarded and violated Plaintiff's and Class Members' privacy rights, and materially harmed them in the process, by failing to establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. Horizon's security deficiencies allowed unauthorized individuals to access, remove from its premises, transport, disclose, and compromise the PII/PHI of hundreds of thousands of individuals—including Plaintiff and Class Members.

50. Horizon's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII/PHI without

[15] Pamela Louis Dolan, "Health Data Breaches Usually Aren't Accidents Anymore," (July 29, 2013), available at http://www.amednews.com/article/20130729/business/130729953/4/ (last visited Dec. 10, 2013).

their knowledge, authorization, and consent. As a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have incurred (and will continue to incur) economic damages and other harm in the form of, *inter alia*: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation.

CLASS ACTION ALLEGATIONS

51. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action as a national class action on behalf of herself and the following Class of similarly situated individuals:

> All persons whose personal identifying information (PII) and personal health information (PHI) were contained on the computers stolen from the Horizon Healthcare Services, Inc.'s Newark, New Jersey, offices on or about November 1, 2013.

Excluded from the Class are (i) Horizon owners, officers, directors, employees, agents, and representatives and its parent entities, subsidiaries, affiliates, successors, and assigns; and (ii) the Court, Court personnel, and members of their immediate families.

52. The putative Class comprises over 839,000 persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

53. The rights of each Class Member were violated in a virtually identical manner as a result of Horizon's willful, reckless, and/or negligent actions and inaction.

54. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Horizon violated FCRA by failing to properly secure Plaintiff's and Class Members' PII/PHI;

b) Whether Horizon violated FCRA by failing to encrypt Plaintiff's and Class Members' PII/PHI in accordance with federal standards;

c) Whether Horizon willfully, recklessly, and/or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PII/PHI;

d) Whether Horizon was negligent in storing Plaintiff's and Class Members' PII/PHI;

e) Whether Horizon owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

f) Whether Horizon breached its duty to exercise reasonable care in protecting and securing Plaintiff's and Class Members' PII/PHI;

g) Whether Horizon was negligent in failing to secure Plaintiff's and Class Members' PII/PHI;

h) Whether by publicly disclosing Plaintiff's and Class Members' PII/PHI without authorization, Horizon invaded Plaintiff's and Class Members' privacy;

i) Whether Horizon has been unjustly enriched in the form of premiums paid by Plaintiff and Class Members that were, in part, paid for the purpose of securing and safeguarding Plaintiff's and Class Members' PII/PHI;

j) Whether Plaintiff and Class Members sustained damages as a result of Horizon's failure to secure and protect their PII/PHI; and

k) Whether Horizon violated federal and state laws by failing to timely notify Plaintiff and Class Members on an individual basis about the theft and dissemination of their PII/PHI.

55. Plaintiff's claims are typical of Class Members' claims in that Plaintiff's claims and Class Members' claims all arise from Horizon's failure to properly safeguard and protect Plaintiff's and Class Members' PII/PHI and the resulting Data Breach.

56. Plaintiff and her counsel will fairly and adequately represent the interests of Class Members. Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiff's attorneys are highly experienced in the prosecution of consumer class actions and data breach class actions, and intend to vigorously prosecute this action on behalf of Plaintiff and Class Members.

57. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class Members have been irreparably harmed as a result of Horizon's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Horizon's failure to secure and protect Plaintiff's and Class Members' PII/PHI.

58. Class certification, therefore, is appropriate pursuant to FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

59. Class certification also is appropriate pursuant to FED. R. CIV. P. 23(b)(2) because Horizon has acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole.

60. Class certification also is appropriate because the expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CLAIMS FOR RELIEF

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

61. The preceding paragraphs are incorporated herein by reference.

62. In enacting FCRA, Congress made several findings, including that "*[t]here is a need to insure* that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and *a respect for the consumer's right to privacy*." 15 U.S.C. § 1681(4) (emphasis added).

63. FCRA requires consumer reporting agencies to *adopt and maintain reasonable procedures* for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner fair and equitable to consumers *while maintaining the confidentiality*, accuracy, relevancy, and proper utilization of such information. 15 U.S.C. § 1681(b).

64. FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

65. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

66. FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681a(i).

67. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.,* 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

68. Plaintiff's PII/PHI constitute Consumer Reports because the information bears on their character, general reputation, personal characteristics, and/or mode of living, and is used and collected by Horizon for the purpose of, *inter alia*, establishing Plaintiff's eligibility for health insurance coverage, payment of health care services for Plaintiff, and establishing rates for Plaintiff's health insurance coverage.

69. Horizon is a Consumer Reporting Agency, as defined under FCRA, because on a cooperative nonprofit basis and/or for monetary fees, Horizon regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing

Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

70. As a Consumer Reporting Agency, Horizon was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiff's and Class Members' PII/PHI) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. *See* 15 U.S.C. § 1681(b).

71. Horizon, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and proximately resulted in the theft of the unsecured and unmonitored laptop computers containing Plaintiff's and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain. In addition to properly securing and monitoring the stolen laptop computers and encrypting Plaintiff's and Class Members' PII/PHI on the computers, Horizon could have (and should have):

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Horizon's locations, (ii) administrative vulnerabilities associated with storing over 839,000 members' PII/PHI on two laptop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Horizon's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the laptop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on unencrypted portable electronic devices.

On information and belief, Horizon took none of these proactive actions to secure the stolen laptop computers and safeguard and protect Plaintiff's and Class Members' PII/PHI, and failed to place itself in a position to immediately notify Plaintiff and Class Members about the Data Breach.

72. Plaintiff's and Class Members' PII/PHI, in whole or in part, constitutes medical information as defined by FCRA. Horizon violated FCRA by failing to specifically protect and limit the dissemination of Plaintiff's and Class Members' PII/PHI (*i.e.*, their medical information) into the public domain.

73. As a direct and proximate result of Horizon's willful and/or reckless violations of FCRA, and the resulting Data Breach, as described above, Plaintiff's and Class Members' unencrypted PII/PHI was taken and made accessible to unauthorized third parties in the public domain.

74. As a direct and proximate result of Horizon's willful and/or reckless violations of FCRA, and the resulting Data Breach, as described above, Plaintiff and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

75. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a

well-established national and international market; (iv) anxiety and emotional distress; (v) statutory damages of not less than $100, and not more than $1000, each; and (vi) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

76. The factual statements and allegations in paragraphs 1–72 of this Complaint are incorporated herein by reference.

77. In the alternative, and as described above, Horizon negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiff's and Class Members' PII/PHI for the permissible purposes outlined by FCRA which, in turn, directly and proximately resulted in the theft of the unsecured and unmonitored laptop computers containing Plaintiff's and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain. In addition to properly securing and monitoring the stolen laptop computers and encrypting Plaintiff's and Class Members' PII/PHI on the computers, Horizon could have (and should have):

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Horizon's locations, (ii) administrative vulnerabilities associated with storing over 839,000 members' PII/PHI on two laptop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data.

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs (roundings), hotline and complaint management—and ensure that these metrics were an integral part of Horizon's corporate governance program.

c) Taken measures to monitor and secure the room and areas where the laptop computers containing the PII/PHI were stored, maintained, and

used, or taken measures to insure that no PII/PHI was stored on unencrypted portable electronic devices.

On information and belief, Horizon took none of these proactive actions to secure and protect Plaintiff's and Class Members' PII/PHI and failed to place itself in a position to immediately notify Plaintiff and Class Members about the Data Breach.

78. It was reasonably foreseeable that Horizon's failure to implement and maintain procedures to safeguard and protect Plaintiff's and Class Members' PII/PHI would result in an unauthorized third party gaining access to their PII/PHI for no permissible purpose under FCRA.

79. As a direct and proximate result of Horizon's negligent violations of FCRA, and the resulting Data Breach, as described above, Plaintiff's and Class Members' PII/PHI was stolen and made accessible to unauthorized third parties in the public domain.

80. As a direct and proximate result of Horizon's negligent violations of FCRA, and the resulting Data Breach, as described above, Plaintiff and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

81. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*: (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III

NEGLIGENCE

82. The factual statements and allegations in paragraphs 1–81 of this Complaint are incorporated herein by reference.

83. Horizon had a duty to exercise reasonable care and caution in safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

84. Horizon violated its duty by failing to exercise reasonable care and caution and safeguard and protect Plaintiff's and Class Members' PII/PHI (as set forth in detail above).

85. It was reasonably foreseeable that Horizon's failure to exercise reasonable care and caution in safeguarding and protecting Plaintiff's and Class Members' PII/PHI would result in an unauthorized third party gaining access to such information for no lawful purpose, particularly where Horizon previously experienced the theft of a laptop containing its insureds' PII/PHI.

86. Plaintiff and Class Members were (and continue to be) damaged as a direct and proximate result of Horizon's failure to secure and protect their PII/PHI in the form of, *inter alia*, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation.

87. Horizon's wrongful actions and inaction (as described above) constituted negligence and/or gross negligence at common law.

COUNT IV

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

88. The factual statements and allegations in paragraphs 1–87 of this Complaint are incorporated herein by reference.

89. Horizon's failure to secure and protect Plaintiff's and Class Members' PII/PHI directly and proximately resulted in the public disclosure of such private information.

90. Dissemination of Plaintiff's and Class Members' PII/PHI is not of a legitimate public concern; publicity of their PII/PHI would be, is and will continue to be offensive to reasonable people.

91. Plaintiff and Class Members were (and continue to be) damaged as a direct and proximate result of Horizon's invasion of their privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI) in the form of, *inter alia*: (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress— for which they are entitled to compensation. At the very least, Plaintiff and Class Members are entitled to nominal damages.

92. Horizon's wrongful actions and inaction (as described above) constituted (and continue to constitute) an ongoing invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI).

COUNT V

UNJUST ENRICHMENT

93. The factual statements and allegations in paragraphs 1–92 of this Complaint are incorporated herein by reference.

94. Plaintiff and Class Members conferred a monetary benefit on Horizon in the form of a portion of the monthly health insurance premiums they paid.

95. Horizon appreciated (and continues to appreciate) such monetary benefit.

96. A portion of the monthly health insurance premiums paid by Plaintiff and Class Members was used to pay for the administrative costs of electronic data management and security services.

97. In light of the Data Breach, and under principles of equity and good conscience, Horizon should not be permitted to retain that portion of the monthly health insurance premiums paid by Plaintiff and Class Members supposedly used to pay for the administrative costs of electronic data management and security that Horizon, in fact, failed to provide.

98. Horizon's retention of these benefits conferred by Plaintiff and Class Members is inequitable.

99. Accordingly, Plaintiff, on behalf of herself and Class Members, seeks to impose a constructive trust over (and recover) all amounts by which Horizon has been (and continues to be) unjustly enriched.

100. Plaintiff and Class Members are entitled to restitution and/or the disgorgement of Horizon's ill-gotten gains under common law.

RELIEF REQUESTED

101. The preceding factual statements and allegations are incorporated herein by reference.

102. **DAMAGES.** As a direct and proximate result of Horizon's wrongful actions and inaction, and the resulting Data Breach (as described above), Plaintiff and Class Members suffered (and continue to suffer) economic damages and other harm in the form of, *inter alia*: (i) the untimely and inadequate notification of the Data Breach; (ii) improper disclosure of their PII/PHI; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (vii) anxiety and emotional distress; and (viii) rights they possess under FCRA—for which they are entitled to compensation. Plaintiff and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and Class Members' damages were foreseeable by Horizon and exceed the minimum jurisdictional limits of this Court.

103. **EXEMPLARY DAMAGES.** Plaintiff and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

104. **INJUNCTIVE RELIEF.** Plaintiff and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring Horizon to, *inter alia*, (i) immediately disclose to Plaintiff and Class Members the precise nature and extent of their PII/PHI contained on the stolen laptop computers, (ii) make prompt and detailed disclosure to all past, present and future patients affected by any future data breaches of their PII/PHI, (iii) immediately encrypt the PII/PHI of its past, present, and future patients, (iv) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any data breaches, (v) submit to periodic compliance audits by a

third party regarding the implementation of and compliance with such policies and procedures, and (vi) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control.

105. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, 15 U.S.C. §§ 1681n(a); o(a).

WHEREFORE, Plaintiff, on behalf of herself and Class Members, respectfully requests that (i) Horizon be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiff be designated the Class Representative, and (iv) Plaintiff's counsel be appointed as Class Counsel. Plaintiff, on behalf of herself and Class Members, further requests that upon final trial or hearing, judgment be awarded against Horizon, in favor of Plaintiff and Class Members, for:

(i) actual damages, consequential damages, FCRA statutory damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

(ii) exemplary damages:

(iii) injunctive relief as set forth above;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

(vi) costs of suit; and

(vii) such other and further relief that the Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, respectfully demand a trial by jury on all of the claims and causes of action so triable.

December 11, 2013

Respectfully submitted,

WILENTZ, GOLDMAN & SPITZER P.A.
90 Woodbridge Center Drive
Suite 900, Box 10
Woodbridge, New Jersey 07095-0958
(732) 636-8000

/s/ Philip A. Tortoreti
Philip A. Tortoreti

Attorneys for Plaintiff

Of Counsel

Ben Barnow
Blake A. Strautins
BARNOW AND ASSOCIATES, P.C.
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com
Email: b.strautins@barnowlaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com